UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

SUE CROFT, COURTNEY BROWN, LINDA SUE DUNN, VIKESHA EXFORD, TIFFANY FARRAND, CHERYL HAYES, DONALD PITCHERS, and MICHELE RUTHERFORD, individually and on behalf of all OTHERS similarly situated,

Plaintiffs,

v.

ASCENSION HEALTH
Defendant.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT – CLASS ACTION

Plaintiffs Sue Croft, Courtney Brown, Linda Sue Dunn, Vikesha Exford, Tiffany Farrand, Cheryl Hayes, Donald Pitchers, and Michele Rutherford (collectively, "Plaintiffs"), by and through the undersigned counsel, bring this class action against Defendant Ascension Health. ("Defendant" or "Ascension"), on behalf of themselves and all others similarly situated (the "Class," defined more fulsomely below). Plaintiffs make the following allegations based on personal knowledge as to their own actions and on information and belief as to all other matters.

NATURE OF THE ACTION

1. As one of the largest private healthcare systems in the United States, Ascension is a cornerstone of healthcare in communities across nineteen states and the District of Columbia. Its network includes 140 hospitals, 40 senior living centers, 35,000 affiliated providers, and

millions of patients.[1] In 2023, Ascension had $28.3 billion in revenue and owned $40.5 billion in assets. Despite its significant resources, Ascension failed to invest in adequate cybersecurity, which resulted in a massive data breach that has harmed millions of people across the United States.

2. Created in 1999 by the merger of two Catholic health systems, Ascension has grown across 25 years of unfettered merger, acquisition, and expansion into a healthcare behemoth responsible for more than 3,000 healthcare facilities across the country—and consequently, the data of tens of millions of current and former patients.

3. Every day, hundreds of thousands of patients across numerous healthcare systems trust Ascension with their health. Many of these individuals have been patients of these facilities and providers long before they were bought up by Ascension. In fiscal year 2023, Ascension facilities hosted 16.4 million doctor's office and clinic visits, 3.1 million emergency room visits, 900,000 virtual provider visits, 599,000 surgeries, 349,000 urgent care visits, and 79,000 births.[2] And every day, in order to access these healthcare services, millions of current and former patients must also trust Ascension with their most sensitive personal information. In May of 2024, Ascension broke that trust.

4. On May 8, 2024, Ascension "detected unusual activity" in its network systems. Computer issues that initially seemed like isolated incidents were quickly discovered to be happening all over the Ascension network across the country. Ascension has not yet disclosed how long hackers had unconstrained access to its systems before their activity was discovered.

---

[1] *About Ascension*, ASCENSION, https://about.ascension.org/about-us (last visited June 8, 2024); *FY23 Ascension Facts & Stats*, ASCENSION, https://about.ascension.org/en/news/media-resources (last visited June 8, 2024).

[2] *FY23 Ascension Facts & Stats*, ASCENSION, https://about.ascension.org/en/news/media-resources (last visited June 8, 2024).

5. Sometime later that same day, a ransomware attack took down Ascension's internal Electronic Health Record system, its online patient portal, and various other systems used to order tests and medications—essentially taking 140 hospital systems across the US entirely offline. To date, the majority of Ascension's facilities remain unable to access their Electronic Health Record system and reliant solely on paper charting for over a month.[3]

6. This attack has since been claimed by Black Basta—a Russian-based ransomware organization well-known for its use of a double extortion tactic, wherein hackers encrypt critical data and vital servers and demand a ransom in exchange for restoring access to the encrypted systems and files, and then further threaten to publish or sell sensitive data on the Dark Web if an additional ransom is not paid.

7. The attack lifecycle for financially motivated hacking groups like Black Basta typically involves identifying the "crown jewels" within a system, accessing and exfiltrating that data, and then deploying ransomware to obfuscate where hackers have been within the system and to create a secondary revenue stream by extorting the entity they attacked.

8. It is extremely rare for hackers to conduct a ransomware attack without exfiltrating data. The immense breadth of this ransomware attack implies the extensive access these hackers had to the data within these systems.

9. Ascension's failure to employ adequate network segmentation ensured that hackers had access to not just one hospital's system but the systems of hundreds of hospitals, outpatient clinics, virtual providers, and senior living facilities across the country.

---

[3] *See Cybersecurity Event Statement*, ASENCION, (June 7, 2024), https://about.ascension.org/en/cybersecurity-event.

10. While Ascension has not yet disclosed the extent of the data accessed and exfiltrated amid this cyberattack (the "Data Breach"), the circumstances suggest the unauthorized disclosure of the Personally Identifiable Information ("PII") and Protected Health Information ("PHI") for potentially millions of current and former Ascension Patients including names, dates of birth, Social Security numbers, patient medical records, prescriptions, diagnoses, and other intimate medical information (collectively, "Private Information").

11. This civil action pursues monetary damages as well as injunctive and declaratory relief from Ascension, stemming from its negligence in safeguarding Plaintiffs' and Class members' Private Information.

12. Ascension systemically collected and maintained vast amounts of Private Information about millions of patients. These patients, including Plaintiffs and Class members, entrusted Ascension with their most sensitive data with the mutual understanding that it would be protected against disclosure. Instead, Ascension's negligence has put millions of current and former patients at lifelong risk of identity theft and fraud.

13. This Data Breach directly resulted from Ascension's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyberattack.

14. After numerous high-profile cyberattacks across the healthcare industry in recent years—including the Change Healthcare breach just three months prior—and numerous warnings by government agencies, such a data breach was a known risk to Ascension. Still, Ascension failed to take the necessary steps to secure Private Information.

15. As a result of the Data Breach, Plaintiffs and Class members suffered concrete injuries in fact including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost

or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

16. Ascension disregarded the rights of Plaintiffs and Class members by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; neglecting to implement standard and reasonably available steps to prevent the Data Breach; and failing to notify Plaintiffs and Class members of the Data Breach promptly and accurately.

17. With the Private Information accessed in the Data Breach, data thieves have already perpetrated identity theft and fraud. Furthermore, they could potentially commit various crimes in the future, such as opening new financial accounts in Class members' names, obtaining loans in Class members' names, using their information to access government benefits, filing fraudulent tax returns, obtaining driver's licenses with Class members' names but another person's photograph, and providing false information to law enforcement during an arrest.

18. Plaintiffs initiate this class action lawsuit on behalf of all those similarly situated to address Ascension's inadequate safeguarding of Class members' Private Information, which it collected and maintained. The lawsuit further aims to hold Ascension accountable for failing to provide timely and adequate notice to Plaintiffs and other Class members regarding the

unauthorized access of their information by an unknown third party and the precise nature of the accessed information.

19. Further, Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

20. Plaintiff Sue Croft is a resident and citizen of Maplesville, Alabama and has been a patient of Ascension St. Vincent Hospital in Clanton, Alabama, where she has received emergency medical care in both 2023 and 2024. Ascension obtained and stored Ms. Croft's Private Information in connection with her treatment at Ascension St. Vincent.

21. Plaintiff Courtney Brown is a resident and citizen of Pensacola, Florida and has been a patient of Ascension since at least 2021. Most recently, she was a patient of Ascension Sacred Heart Urgent Care Center at Pensacola on May 8, 2024 and at Ascension Sacred Heart Hospital from May 8-9, 2024. Ascension obtained and stored Ms. Brown's Private Information in connection with her treatment at Ascension Sacred Heart facilities since 2021.

22. Plaintiff Linda Sue Dunn is a resident and citizen of Mountain Home, Arkansas and a former patient of Ascension Sacred Heart Hospital in Pensacola, Florida and Milton, Florida where she received medical treatment from at least April 2023 until March 2024. Ascension obtained and stored Ms. Moris-Dunn's Private Information in connection with her treatment at Ascension Sacred Heart Hospital.

23. Plaintiff Vikesha Exford is a resident and citizen of Midfield, Alabama and has been a patient of Ascension St. Vincent facilities for over ten years. Ascencion obtained and stored

Ms. Exford's Private Information in connection with her treatment at Ascension St. Vincent facilities.

24. Plaintiff Tiffany Farrand is a resident and citizen of Milwaukee, Wisconsin and has been a patient of Ascension since at least 1999. Ascension obtained and stored Ms. Farrand's Private Information in connection with her treatment at Ascension St. Francis and Ascension St. Joseph facilities.

25. Plaintiff Cheryl Hayes is a resident and citizen of Tulsa, Oklahoma and has been a patient of Ascension St. John Medical Center, receiving ongoing medical care since May 2022. Ascension obtained and stored Ms. Hayes's Private Information in connection with her treatment at Ascension St. John Medical Center.

26. Plaintiff Donald Pitchers is a resident and citizen of Evansville, Indiana and has been a patient of multiple Ascension facilities, receiving ongoing medical care since approximately 2019. Ascension obtained and stored Mr. Pitchers's Private Information in connection with his treatment at Ascension Northside Crossing, Ascension St. Vincent Hospital, and an Ascension clinic at his workplace.

27. Plaintiff Michele Rutherford is a resident and citizen of Wichita, Kansas and has been a patient of Ascension Via Christi, receiving ongoing medical care since May of 2023 Ascension obtained and stored Ms. Rutherford's Private Information in connection with her treatment at Ascension Via Christi facilities.

28. Defendant Ascension Health is a non-profit corporation properly recognized and sanctioned by the laws of the State of Missouri, with its headquarters located at 4600 Edmundson Road, St., St. Louis, Missouri 63134, in the County of St. Louis. Ascension is the largest non-profit, Catholic health-system in the United States that "includes approximately 134,000

associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia."[4]

JURISDICTION AND VENUE

29. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiffs (and many members of the proposed Class) are citizens of states different from Defendant.

30. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. The Defendant's principal place of business is located within this District, indicating a deliberate engagement with the markets here. Consequently, the exercise of jurisdiction by this Court is not only justified but also appropriate, given the Defendant's intentional involvement in this District's economic activities.

31. Venue is proper pursuant to 28 U.S.C. § 1391(a)(1) due to the Defendant's principal place of business being situated within this District. Moreover, a significant portion of the events and omissions that form the basis of this action transpired within this District. Hence, it is fitting that this Court serves as the venue for adjudicating this matter.

[4] *About Ascension*, ASCENSION, https://about.ascension.org/about-us (last visited June 3, 2024).

FACTUAL ALLEGATIONS

Ascension's Business and Privacy Practices

32. Ascension is a Catholic health system comprising approximately 134,000 associates, 35,000 affiliated providers, and 140 hospitals. Its services span across communities in 19 states and the District of Columbia.[5]

33. Plaintiffs and Class members are individuals who are both current and former patients of Ascension.

34. During their interactions with Ascension, Plaintiffs and Class members entrusted Ascension with their sensitive Private Information.

35. As part of the process of collecting Private Information from patients, including Plaintiffs, Ascension pledged to ensure confidentiality and adequate security for the data it gathered from patients. This commitment was articulated through its relevant privacy policy and other disclosures, adhering to statutory privacy requirements.

36. Indeed, Defendant asserts on its website that: "[t]he Site has security measures in place to protect against the loss, misuse, or alteration of information under Our control."[6]

37. Plaintiffs and the Class members trusted these assurances and counted on this sophisticated business entity to maintain the confidentiality and security of their sensitive Private Information. They expected Ascension to use this information solely for business purposes and to make only authorized disclosures. Patients, in general, insist on security measures to protect their Private Information, particularly when it involves sensitive details like Social Security numbers.

---

[5] *About Ascension,* ASCENSION, https://about.ascension.org/about-us (last visited June 3, 2024).
[6] *Website Privacy Policy,* ASCENSION, https://about.ascension.org/privacy (last visited June 7, 2024).

The Data Breach

38. In or about May 2024, Ascension posted a notice to its website (the "Online Notice"), informing Plaintiffs and Class members that:

> On Wednesday, May 8, we detected unusual activity on select technology network systems, which we now believe is due to a cybersecurity event. At this time we continue to investigate the situation. We responded immediately, initiated our investigation and activated our remediation efforts. Access to some systems have been interrupted as this process continues.
>
> Our care teams are trained for these kinds of disruptions and have initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible. There has been a disruption to clinical operations, and we continue to assess the impact and duration of the disruption.
>
> We have engaged Mandiant, a third party expert, to assist in the investigation and remediation process, and we have notified the appropriate authorities. Together, we are working to fully investigate what information, if any, may have been affected by the situation. Should we determine that any sensitive information was affected, we will notify and support those individuals in accordance with all relevant regulatory and legal guidelines.[7]

39. The Online Notice failed to include crucial information such as the date(s) of the Data Breach, the identity of the cybercriminals responsible, the specifics regarding the root cause of the breach, the vulnerabilities exploited, and the remedial actions taken to prevent future breaches. To this day, these critical details have not been explained or clarified to Plaintiffs and Class members, who maintain a vested interest in safeguarding their Private Information. Without such essential details, the ability of Plaintiffs and Class members to effectively mitigate the resulting harms is significantly compromised.

40. Despite the intentional opacity from Ascension regarding the root cause of this incident, the Online Notice provides several discernible facts: a) the Data Breach was perpetrated by cybercriminals; b) these cybercriminals initially breached Ascension's networks and systems,

---

[7] *Network Interruption Update*, ASCENSION, (May 9, 2024), https://about.ascension.org/news/2024/05/network-interruption-update2.

subsequently exfiltrating data, colloquially termed as "stealing" data; and c) within Ascension's networks and systems, the cybercriminals specifically targeted information—potentially including Plaintiffs' and Class members' PHI, PII, and other sensitive data—for download and theft.

41. Ascension's Online Notice further fails to state whether any efforts were made to reach the individuals whose data was compromised in the Data Breach. To date, Plaintiffs have not received notice from Ascension.

42. On information and belief, the information compromised in the Data Breach included Plaintiffs' and Class members' PII and PHI as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

43. As detailed further below, Ascension was bound by various obligations stemming from the FTC Act, HIPAA, contractual agreements, common law principles, and industry standards to maintain the confidentiality of Plaintiffs' and Class members' Private Information and safeguard it against unauthorized access and disclosure.

44. Ascension failed to implement reasonable security procedures and practices commensurate with the sensitivity of the information entrusted to them by Plaintiffs and Class members. This lapse led to the exposure of Private Information, which could have been mitigated through measures such as encryption or timely deletion when the information was no longer required.

45. The attacker successfully accessed and obtained files containing unencrypted Private Information belonging to Plaintiffs and Class members. As a result of the Data Breach, Private Information belonging to Plaintiffs and Class members was compromised and stolen.

46. Plaintiffs further hold the belief that both their own Private Information and that of the Class were subsequently sold on the dark web in the aftermath of the Data Breach. This assertion aligns with the typical modus operandi of cybercriminals who engage in such cyber-attacks.

Ascension Acquired, Collected, and Stored Patients' Private Information

47. Ascension acquires, collects, and stores massive amounts of Private Information on its current and former patients.

48. As a condition of becoming a patient of or purchasing medical supplies from Ascension, Ascension requires that patients (and other personnel) entrust it with highly sensitive personal information.

49. By obtaining, collecting, and using Plaintiffs' and Class members' Private Information, Ascension assumed legal and equitable duties to protect such information. Ascension knew or should have known that it was responsible for protecting this Private Information from disclosure.

50. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Ascension absent a promise to safeguard this information from unauthorized disclosure.

51. During the process of collecting Private Information from patients, including Plaintiffs and Class members, Ascension purportedly pledged to ensure confidentiality and adequate security for their data. This commitment was purportedly articulated through its relevant privacy policy and other disclosures, in adherence to statutory privacy mandates.

52. Ascension's website states: "that: "[t]he Site has security measures in place to protect against the loss, misuse or alteration of information under Our control."[8]

53. Plaintiffs and Class members relied on Ascension to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

54. The injuries to Plaintiffs and Class members were directly and proximately caused by Ascension's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

55. The ramifications of Ascension's failure to properly secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private information is stolen, fraudulent use of that information and resulting damage to victims may continue for years.

56. As a healthcare entity in custody of the Private Information of its patients, Ascension knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of a breach. Ascension failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Plaintiffs' Private Information Has Value

57. Criminal actors highly value PHI and PII. Such information is continually traded on underground "dark web" marketplaces that cannot be accessed through standard web browsers.

[8] *Website Privacy Policy*, Ascensio, https://about.ascension.org/privacy (last visited June 7, 2024).

58. Private Information can be sold at a price ranging from $40 to $200.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

59. The kind of information likely exposed in the Data Breach is of much higher value than simple credit card information, which customers can change or close accounts.[11] By contrast the PII exposed in the Data breach cannot readily be changed—*e.g.*, addresses and Social Security numbers.

60. Social Security numbers—which, according to available information, were almost certainly compromised for some Plaintiffs and Class members in the Data Breach—are one of the most detrimental forms of Private Information to have stolen due to the multitude of fraudulent purposes for which they can be used and the significant challenge individuals face in changing them.

61. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."[12] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[13]

---

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[10] *In the Dark*, VPNOverview, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 7, 204).

[11] *See* Jesse Damiani, *Your Social Security Number Costs $4 on the Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-darkweb-new-report-finds/?sh=770cee3a13f1.

[12] *See Avoid Identity Theft: Protect Social Security Numbers*, Soc. Sec. Phila. Reg., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited June 7, 2024).

[13] *Id.*

62. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

63. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

64. Theft of PHI, which, upon information and belief, was compromised in the Data Breach, is also gravely serious, putting patients at risk of medical identity theft wherein "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[15]

65. A study conducted by Experian revealed that the average cost of medical identity theft per incident is approximately $20,000. Additionally, the majority of victims of medical identity theft are compelled to cover out-of-pocket expenses for healthcare services they did not receive in order to reinstate their coverage. Furthermore, almost half of medical identity theft victims lose their healthcare coverage following the incident, while nearly one-third experience

---

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015, 4:59 AM), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

[15] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited June 7, 2024).

an increase in insurance premiums. Alarmingly, 40 percent of victims are unable to fully resolve their identity theft ordeal.[16]

66. Moreover, fraudulent medical treatment can have non-financial impacts. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because their medical records contain information supplied by an individual obtaining treatment under a false name.[17]

67. Further, loss of personal health information, such as treatment history, diagnoses, and prescription information, exposes the victims to loss of reputation, loss of employment, blackmail, and other harms including the trauma of having your most personal details published online for all to see.

68. PII also sells on legitimate markets, an industry that is valued at hundreds of billions of dollars per year. Customers themselves are able to sell non-public information directly to data brokers who aggregate the information for sale to marketers or others. Consumers may also sell their web browsing histories to the Nielson Corporation for up to $50 annually.

69. Because their Private Information has value, Plaintiffs and Class members must take significant protective measures, including years of constant surveillance of their financial and personal records, credit monitoring, and identity protection.

---

[16] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, (March 31, 2023), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-themand-what-to-do-after-one/.

[17] *See 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse*, WASH. POST, Andrea Peterson, Mar. 20, 2015, available at http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 10, 2016).

Ascension Could Have Foreseen and Prevented the Data Breach

70. Nothing about this attack was extraordinary. Cybercriminals target the healthcare industry the most due to the treasure trove of confidential health and personal information maintained and stored by healthcare organizations.

71. Cyberattacks doubled from 2016 to 2021 and have resulted in the exposure of personal health information for approximately 42 million patients.[18] In 2023 alone, the FBI reported 249 ransomware attacks in the healthcare industry.[19]

72. Cyberattacks against the healthcare industry in particular have been common for over a decade, with the FBI warning as early as 2011 that cybercriminals targeting healthcare providers and others were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII."[20]

73. The FBI again warned healthcare stakeholders in 2014 that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[21]

---

[18] *See Healthcare Data Breaches: Insights and Implications,* Nat'l Libr. Of Med. (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-..

[19] *See Health industry struggles to recover from cyberattack on a unit of United Health,* NPR (Mar. 9, 2024, 7:00 AM), https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united.

[20] Gordon M. Snow, FBI, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, The FBI Testimony (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector .

[21] *See FBI Cyber Bulletin: Malicious Actors Targeting Protected Health Information,* Federal Bureau of Investigation (Aug. 19, 2014) https://publicintelligence.net/fbi-targeting-healthcare20(PII).

74. In 2017, the Department of Health and Human Services released a ransomware Fact Sheet. This document made it clear to entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[22]

75. Additionally, in light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including Change Healthcare (potentially hundreds of millions of patients, March 2024), HCA Healthcare (11-million patients, July 2023), Managed Care of North America (8-million patients, March 2023), PharMerica Corporation (5-million patients, March 2023), HealthEC LLC (4-million patients, July 2023), ESO Solutions, Inc. (2.7-million patients, September 2023), Prospect Medical Holdings, Inc. (1.3-million patients, July-August 2023), Ascension knew or should have known that its electronic records would be targeted by cybercriminals.

76. According to an article in the HIPAA Journal posted on November 2, 2023, cybercriminals hack into healthcare networks for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights]

[22] *See Fact Sheet: Ransomware and HIPAA,* U.S. Dep't. of Health & Hum. Serv's., https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited June 7, 2024).

OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[23]

77. Under the HIPAA Privacy Rules, a breach is defined as, "[t]he acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[24] Accordingly, an attack such as the one that was discovered on or about May 8, 2023 is considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule.

78. Such an attack is also considered a "Security Incident" under HIPAA. Under the HIPAA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304. According to the Department of Health and Human Services, "[t]he presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."[25]

79. Data Breaches can be prevented. Cybersecurity professionals and applicable information security standards urge organizations to take reasonable technical and administrative information security controls. Commonly recommended controls include:: ensuring computer networks are adequately segmented, implementing and configuring intrusion prevention and detection technologies, monitoring computer systems using appropriate tools and responding to

---

[23] Steve Alder, , *Editorial: Why Do Criminals Target Medical Records*, The HIPAA J. (Nov. 2, 2023),https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[24] *See Breach Notification Rule*, U.S. Dep't of Health & Hum. Serv's, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited June 7, 2024).
[25] *See Fact Sheet: Ransomware and HIPAA,* U.S. Dep't of Health & Hum. Serv's, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet (last visited June 7, 2024).

alerts on suspicious behavior, implementing spam and malware filters, requiring multifactor authentication for external access, implementing secure cryptographic algorithms, timely applying security patches and updates, limiting the use of privileged or administrative accounts, training employees on the handling of suspicious emails, implementing an effective vulnerability management program, ensuring vendors implement and maintain adequate security controls, and implementing heightened security controls around sensitive data sources.

80. The Data Breach underscores Ascension's failure to sufficiently implement one or more vital security measures aimed at preventing cyberattacks. The Data Breach never would have occurred without Ascension's inadequate cybersecurity controls, enabling data thieves to access and acquire the Private Information of, according to available information, thousands to tens of thousands of individuals, including Plaintiffs and Class members.

81. Ascension knew that unprotected or exposed Private Information in the custody of healthcare companies is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

82. At all relevant times, Ascension knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members and of the foreseeable consequences that would occur if Ascension's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

83. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Ascension Did Not Comply with Federal Law and Regulatory Guidance

Ascension did not comply with FTC Guidelines

84. The United States government issues guidelines for businesses that store sensitive data to help them minimize the risks of a data breach. The FTC publishes guides for businesses about the importance of reasonable data security practices.[26] One of its publications sets forth data security principles and practices for businesses to protect sensitive data.[27] The FTC tells businesses to (a) protect the personal information they collect and store; (b) dispose of personal information it no longer needs; (c) encrypt information on their networks; (d) understand their network's vulnerabilities; (e) put policies in place to correct security problems. The FTC recommends businesses use an intrusion detection system, monitor networks for large, outgoing data transmissions, monitor incoming traffic for unusual activity, and make a plan in case a breach occurs.[28]

85. Further, the FTC tells organizations to limit access to sensitive data, require the use of complex passwords on networks, use industry-tested security methods; and verify the use of reasonable security measures by third-party service providers.[29]

86. The FTC brings enforcement actions against businesses that fail to reasonably protect customer information. The Commission treats the failure to use reasonable care and appropriate measures to protect against unauthorized access to confidential customer data as an

---

[26] *Start with Security: A Guide for Business*, Fed. Trade Comm'n. (2023), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited June. 7, 2024).

[27] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (2016), https://www.ftc.gov/businessguidance/resources/protecting-personal-informationguide-business (last visited June 7, 2024).

[28] *Id.*

[29] Fed. Trade Comm'n. *supra* note 26.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders issued in these actions state the measures required for businesses to meet their data security obligations.[30]

87. These FTC enforcement actions include actions against healthcare providers like Ascension. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

88. Ascension knew of its obligation to implement and use basic data security practices to protect to Plaintiffs' and Class members' Private properly.

89. Still, Ascension failed to comply with those recommendations and guidelines, which if followed would have prevented the Data Breach. This failure to reasonably protect against unauthorized access to Private Information is an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Ascension's failure to protect Plaintiffs' and Class members' Private Information suggests its failure to comply fully with standard cybersecurity practices such as those described above.

Ascension did not comply with HIPAA Guidelines

91. Ascension is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and

[30] Privacy and Security Enforcement, Fed. Trade Comm'n., https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited June 7, 2024).

Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

92. Ascension is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").37 See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

93. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

94. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

95. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

96. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

97. HIPAA's Security Rule mandates that Ascension:

a. Safeguard the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate;

b. Shield against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Guard against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

98. HIPAA further requires Ascension to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

99. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

100. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Ascension to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[31]

101. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the

[31] *Breach Notification Rule*, U.S. Dep't of Health & Hum. Serv's, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed June 7, 2024).

covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

102. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

103. HIPAA also requires the Office for Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.39 The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[32]

Ascension did not comply with Industry Standards

104. As discussed in depth above, experts in cybersecurity frequently highlight healthcare entities as particularly vulnerable to cyberattacks due to the high value of the Private Information they collect and maintain.

---

[32] *Guidance on Risk Analysis,* U.S. Dep't. of Health & Hum. Serv's. (2019), https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es.

105. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Ascension, including: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Ascension failed to follow these industry best practices, including a failure to implement multi-factor authentication.

106. Standard cybersecurity practices for healthcare entities include installing robust malware detection software, monitoring and limiting network ports, securing web browsers and email systems, setting up firewalls, switches, and routers, and ensuring physical security systems are protected. Additionally, it is essential to safeguard communication systems and train staff on critical security protocols. Ascension failed to adhere to these best practices, including neglecting to properly train staff.

107. Ascension failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, the Center for Internet Security's Critical Security Controls (CIS CSC), and the HITRUST CSF, which are all established standards in reasonable cybersecurity readiness.

108. The aforementioned frameworks represent established industry standards for healthcare entities. Had Ascension complied with these accepted standards, the hackers would not have been able to exploit Ascension's vulnerabilities and carry out the Data Breach.

The Ascension Data Breach Harmed Plaintiffs and Class Members

109. As a result of Ascension's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the hands of

criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is imminent. Consequently, Plaintiffs and Class members have sustained actual and imminent injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the effects of the Data Breach; (v) loss of benefit of the bargain; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk to their Private Information, which remains unencrypted and accessible to unauthorized third parties and is still backed up in Ascension's possession, subject to further unauthorized disclosures unless Ascension implements appropriate and adequate protective measures.

110. The unencrypted Private Information of Plaintiffs and Class members will almost certainly end up being distributed through illicit underground criminal networks, including being sold on the dark web, as that is the modus operandi of hackers. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members. Simply put, unauthorized individuals could easily access the Private Information of Plaintiffs and Class members.

111. As a result of the Data Breach, hackers can now commit identity theft, financial fraud, and other fraud against Plaintiffs and Class members, given the stolen Private Information's sensitive nature. Plaintiffs and Class members therefore have suffered injury and face an imminent, substantial risk of further injuries like identity theft and related cybercrimes.

112. The Private Information likely exposed in the Data Breach is highly valuable and sought after on illicit underground markets for use in committing identity theft and fraud. Malicious actors use this data to access bank accounts, credit cards, and social media accounts,

among other things. They may also use the Private Information to open new financial or utility accounts, seek medical treatment using victims' insurance, file fraudulent tax returns, seek and obtain government benefits or government IDs, or create new identities for use in committing frauds. Because victims of breaches can become less diligent in account monitoring over time, bad actors may wait years before using the Private Information, or they may re-use it to commit several cybercrimes.

113. Even where individuals receive reimbursement for resulting financial losses, they are not made whole again because of the significant time and effort required to do so. The Government Accountability Office reported that criminals often hold onto stolen data for more than a year after it is obtained, waiting for victims to become less vigilant before using the data to commit identity theft. And fraudulent use of data may continue for years after its sale or publication. The GAO concluded that studies that try to measure harms from data breaches "cannot necessarily rule out all future harm."[33]

114. The Identity Theft Resource Center's 2021 survey reported that victims of identity theft reported suffering negative experiences and emotional harms: anxiety (84%); feelings of violation (76%); rejection for credit or loans (83%); financial related identity problems (32%); resulting problems with family members (32%); feeling suicidal (10%).[34]

115. Physical harms also result from identity theft. A similar survey found that victims suffered resulting physical symptoms: sleep disturbances (48.3%); inability to concentrate / lack

---

[33] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, U.S. GOV'T. ACCOUNTABILITY OFF., http://www.gao.gov/new.items/d07737.pdf (last visited June 7, 2024) ("GAO Report").

[34] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/wpcontent/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf.

of focus (37.1%); inability to work because of physical symptoms (28.7%); new physical illnesses including stomach problems, pain, and heart palpitations (23.1%); starting or relapsing into unhealthy or addictive behaviors (12.6%).[35]

116. Theft of PHI carries significant consequences. A thief could potentially exploit your identity or health insurance details to seek medical treatment, obtain prescription medications, submit claims to your insurance provider, or access other healthcare services. If the thief's health information becomes intertwined with data breach victim's, it could impact victim's medical treatment, insurance coverage, payment records, and even victim's credit report.

117. Unauthorized disclosure of sensitive Private Information also reduces its value to its rightful owner, as recognized by courts as an independent source of harm.[36] PII and PHI constitute valuable property rights.[37]

118. Even consumers who have been victims of previous data breaches are injured when their data is stolen and traded. Each data breach increases the likelihood that the victim's personal information will be exposed on the dark web to more individuals who are looking to misuse it.

119. Because of these injuries resulting from the Data Breach, Plaintiffs and Class members suffer and continue to suffer economic loss and actual harm, including:

- disclosure or confidential information to a third party without consent;

---

[35] *Identity Theft: The Aftermath 2017*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited June 7, 2024).

[36] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[37] *See* U.S. GOV. ACCOUNTABILITY OFF., *supra* note 33.

- loss of the value of explicit and implicit promises of data security;
- identity fraud and theft; anxiety, loss of privacy, and emotional distress;
- the cost of detection and prevention measures for identity theft and unauthorized financial account use;
- lowered credit scores from credit inquiries; unauthorized charges;
- diminution of value of PII and PHI;
- loss of use of financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amounts they were permitted to obtain from accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- costs of credit monitoring, identity theft production services, and credit freezes;
- costs associated with loss of time or productivity or enjoyment of one's life from the time required to mitigate and address consequences and future consequences of the Data Breach, such as searching for fraudulent activity, imposing withdrawal and purchase limits, as well as the stress and nuisance of Data Breach repercussions;
- imminent, continued, and certainly impending injury flowing from the potential fraud and identity theft posed by the unauthorized possession of data by third parties.

120. Plaintiffs and Class members place a significant value on data security. About half of consumers consider data security to be a main or important consideration in their purchasing decision and would be willing to pay more to work with those with better data security. Likewise,

70% of consumers would provide less personal information to organizations that suffered a data breach.[38]

Victims Have Lost the Benefit of the Bargain

121. Furthermore, Ascension's poor data security practices deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Ascension and/or its agents for the provision of medical services, Plaintiffs and other reasonable patients understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information, when in fact, Ascension did not provide the expected data security. Accordingly, Plaintiffs and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Ascension's.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

122. Considering the nature of the targeted attack in this case, involving sophisticated criminal activity and the sensitive Private Information at stake, there is a high likelihood that entire datasets of stolen information have either been or will be circulated on the black market or dark web. Criminals intend to exploit this Private Information for identity theft crimes, such as opening bank accounts in victims' names for purchases or money laundering, filing fraudulent tax returns, securing loans or lines of credit, or submitting false unemployment claims.

123. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

[38] *Beyond the Bottom Line: The Real Cost of Data Breaches*, FIREEYE, p. 14, (May, 2016), https://web.archive.org/web/20230628100935/https://www2.fireeye.com/rs/848-DID-242/images/rpt-beyond-bottomline.pdf.

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. Consequently, Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

125. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per individual. This is reasonable and necessary cost to monitor to protect Plaintiffs and Class members from the risk of identity theft that arose from Defendant's Data Breach.

Allegations Relating to Plaintiffs

Plaintiff Courtney Brown's Experience

126. Plaintiff Courtney Brown is an Ascension patient who has obtained services from Ascension Sacred Heart medical facilities since at least 2021, and most recently on May 8-9, 2024 at Ascension Sacred Heart Hospital.

127. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension Sacred Heart medical facilities.

128. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Browm's Private Information in its system.

129. Plaintiff Brown learned of the Data Breach not from ascension directly but from coworkers who were discussing the breach.

130. Plaintiff Brown works in healthcare and knows the importance of keeping patient information confidential.

131. Plaintiff Brown is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or

any other unsecured source. Plaintiff Brown would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

132. Upon information and belief, Plaintiff Brown's Private Information was compromised in the Data Breach.

133. In response to the Data Breach, Plaintiff Brown diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

134. Plaintiff Brown has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

135. The Data Breach has caused Plaintiff Brown to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

136. As a result of the Data Breach, Plaintiff Brown anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

137. As a result of the Data Breach, Plaintiff Brown is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

138. Plaintiff Brown has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Sue Croft's Experience

139. Plaintiff Sue Croft is an Ascension patient who has obtained services from Ascension St. Vincent Hospital there in or about 2023 and 2024.

140. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension St. Vincent Hospital.

141. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Croft's Private Information in its system.

142. Plaintiff Croft learned of the Data Breach not from ascension directly but from browsing her Facebook feed.

143. Plaintiff Croft is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any

other unsecured source. Plaintiff Croft would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

144. Upon information and belief, Plaintiff Croft's Private Information was compromised in the Data Breach.

145. In response to the Data Breach, Plaintiff Croft diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

146. Plaintiff Croft has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

147. The Data Breach has caused Plaintiff Croft to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff Croft anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

149. As a result of the Data Breach, Plaintiff Croft is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

150. Plaintiff Croft has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Linda Sue Dunn's Experience

151. Plaintiff Linda Sue Dunn is a former Ascension patient who obtained services from Ascension Sacred Heart Hospital facilities in Milton, Florida and Pensacola, Florida there in or about April 2023 through March 2024.

152. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension Sacred Heart Hospital.

153. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Dunn's Private Information in its system.

154. Plaintiff Dunn learned of the Data Breach not from Ascension but from browsing online.

155. Plaintiff Dunn is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has

never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Dunn would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

156. Upon information and belief, Plaintiff Dunn's Private Information was compromised in the Data Breach.

157. In response to the Data Breach, Plaintiff Dunn diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

158. Plaintiff Dunn has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

159. The Data Breach has caused Plaintiff Dunn to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

160. As a result of the Data Breach, Plaintiff Dunn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

161. As a result of the Data Breach, Plaintiff Dunn is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

162. Plaintiff Dunn has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Vikesha Exford's Experience

163. Plaintiff Vikesha Exford is an Ascension patient who has obtained services from Ascension St. Vincent medical facilities for over ten years, including at an Ascension St. Vincent outpatient clinic in Gardendale, Alabama and at Ascension St. Vincent Hospital in Birmingham, Alabama.

164. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension St. Vincent facilities.

165. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Exford's Private Information in its system.

166. Plaintiff Exford learned of the Data Breach not from ascension directly but while browsing online.

167. Plaintiff Exford is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Exford would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

168. Upon information and belief, Plaintiff Exford's Private Information was compromised in the Data Breach.

169. In response to the Data Breach, Plaintiff Exford diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

170. Plaintiff Exford has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to

further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

171. The Data Breach has caused Plaintiff Exford to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

172. As a result of the Data Breach, Plaintiff Exford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

173. As a result of the Data Breach, Plaintiff Exford is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

174. Plaintiff Exford has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Tiffany Farrand's Experience

175. Plaintiff Tiffany Farrand is an Ascension patient who has been receiving ongoing medical care from Ascension in Milwaukee, Wisconsin since at least 1999.

176. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension St. Francis and Ascension St. Joseph facilities.

177. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Farrand's Private Information in its system.

178. Plaintiff Farrand learned of the Data Breach not from Ascension but by hearing about it on the news.

179. Plaintiff Farrand is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Farrand would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

180. Upon information and belief, Plaintiff Farrand's Private Information was compromised in the Data Breach.

181. In response to the Data Breach, Plaintiff Farrand diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

182. Plaintiff Farrand has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to

further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

183. The Data Breach has caused Plaintiff Farrand to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

184. As a result of the Data Breach, Plaintiff Farrand anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

185. As a result of the Data Breach, Plaintiff Farrand is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

186. Plaintiff Farrand has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Cheryl Hayes's Experience

187. Plaintiff Cheryl Hayes is an Ascension patient who has been receiving ongoing medical care from Ascension St. John Medical Center since May 2022.

188. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension St. John Medical Center.

189. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Hayes's Private Information in its system.

190. Plaintiff Hayes learned of the Data Breach not from Ascension but by word-of-mouth from other impacted individuals.

191. Plaintiff Hayes is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Hayes would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

192. Upon information and belief, Plaintiff Hayes's Private Information was compromised in the Data Breach.

193. In response to the Data Breach, Plaintiff Hayes diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

194. Plaintiff Hayes has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to

further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

195. The Data Breach has caused Plaintiff Hayes to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

196. As a result of the Data Breach, Plaintiff Hayes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

197. As a result of the Data Breach, Plaintiff Hayes is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

198. Plaintiff Hayes has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Donald Pitchers's Experience

199. Plaintiff Donald Pitchers is an Ascension patient who has been receiving ongoing medical care from Ascension facilities since approximately 2019.

200. He was required to provide his Private Information to Ascension as a condition to receiving medical services at Ascension Northside Crossing Primary Care, Ascension St. Vincent Hospital in Evansville, Indiana, and an Ascension clinic at his workplace.

201. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Pitchers's Private Information in its system.

202. Plaintiff Pitchers first learned of the Data Breach not from Ascension but from the local news.

203. Plaintiff Pitchers is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Pitchers would not have entrusted his Private Information to Ascension had he known of Ascension's lax data security policies.

204. Upon information and belief, Plaintiff Pitchers's Private Information was compromised in the Data Breach.

205. In response to the Data Breach, Plaintiff Pitchers diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. He has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

206. Plaintiff Pitchers has suffered tangible harm resulting from the compromise of his Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of his Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to

further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

207. The Data Breach has caused Plaintiff Pitchers to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed him of key details about the Data Breach's occurrence.

208. As a result of the Data Breach, Plaintiff Pitchers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

209. As a result of the Data Breach, Plaintiff Pitchers is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

210. Plaintiff Pitchers has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

Plaintiff Michele Rutherford's Experience

211. Plaintiff Michele Rutherford is an Ascension patient who has been receiving ongoing medical care from Ascension Via Christi in Wichita, Kansas since approximately May 2023.

212. She was required to provide her Private Information to Ascension as a condition to receiving medical services at Ascension Via Christi facilities.

213. Upon information and belief, at the time of the Data Breach, Ascension maintained Plaintiff Rutherford's Private Information in its system.

214. Plaintiff Rutherford learned of the Data Breach not from Ascension but by seeing information about the ransomware attack on the local news.

215. Plaintiff Rutherford is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Rutherford would not have entrusted her Private Information to Ascension had she known of Ascension's lax data security policies.

216. Upon information and belief, Plaintiff Rutherford's Private Information was compromised in the Data Breach.

217. In response to the Data Breach, Plaintiff Rutherford diligently undertook measures to mitigate its effects. This included thorough research to confirm the breach's authenticity and continuous monitoring of financial accounts for any suspicious transactions, which may remain undetected for years. She has invested considerable time addressing the fallout of the breach—time that would have otherwise been allocated to work or leisure activities. Regrettably, the time is irretrievably lost and cannot be reclaimed.

218. Plaintiff Rutherford has suffered tangible harm resulting from the compromise of her Private Information due to the Data Breach, including: (i) an invasion of privacy; (ii) the unlawful appropriation of her Private Information; (iii) a reduction or loss in the value of Private Information; (iv) expended time and opportunity costs incurred in mitigating the actual repercussions of the Data Breach; (v) the forfeiture of expected benefits from the agreement; (vi) forgone opportunity costs related to mitigating the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) enduring and potentially escalating exposure of her Private Information to risk, while it remains unencrypted and susceptible to unauthorized access and misuse by third parties, and while it remains within Ascension's possession, subject to

further unauthorized disclosure until appropriate and sufficient protective measures are implemented.

219. The Data Breach has caused Plaintiff Rutherford to suffer fear, anxiety, and stress, which has been compounded by the fact that Ascension has still not fully informed her of key details about the Data Breach's occurrence.

220. As a result of the Data Breach, Plaintiff Rutherford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

221. As a result of the Data Breach, Plaintiff Rutherford is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

222. Plaintiff Rutherford has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Ascension's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

223. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs propose the following "Class" definition, subject to amendment as appropriate:

> **Nationwide Class:**
> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Class").

224. Plaintiffs also seek certification of the following statewide subclasses, defined as follows and subject to amendment as appropriate:

Arkansas Subclass:
All Arkansas residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Arkansas Subclass").

Florida Subclass:
All Florida residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Florida Subclass").

Indiana Subclass:
All Indiana residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Indiana Subclass").

Kansas Subclass:
All Kansas residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Kansas Subclass").

Oklahoma Subclass:
All Oklahoma residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Oklahoma Subclass").

Wisconsin Subclass:
All Wisconsin residents whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach that Defendant disclosed in or about May 2024 (the "Wisconsin Subclass").

225. Excluded from the Class are the following individuals and/or entities: Ascension and Ascension's parents, subsidiaries, affiliates, officers and directors, and any entity in which Ascension has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, members of their immediate families, and chambers staff.

226. Plaintiffs reserve the right to amend the definitions of the Class or add additional Classes or Subclasses.

227. Numerosity: The patients of the Class are so numerous that joinder of all patients is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Ascension, upon information and belief, thousands of individuals were impacted. The Class is identifiable within Ascension's records, and these individuals will be identified when Ascension completes its full review of the files that were impacted.

228. Commonality: Common questions of law and fact exist as to all patients of the Class and predominate over any questions affecting solely individual patients of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Ascension had a duty to protect the Private Information of Plaintiffs and Class members;

b. Whether Ascension had respective duties not to disclose the Private Information of Plaintiffs and Class members to unauthorized third parties;

c. Whether Ascension had respective duties not to use the Private Information of Plaintiffs and Class members for non-business purposes;

d. Whether Ascension failed to adequately safeguard the Private Information of Plaintiffs and Class members;

e. Whether and when Ascension actually learned of the Data Breach;

f. Whether Ascension adequately, promptly, and accurately informed Plaintiffs and Class members that their Private Information had been compromised;

g. Whether Ascension violated the law by failing to promptly notify Plaintiffs and Class members that their Private Information had been compromised;

h. Whether Ascension failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Ascension adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Ascension's wrongful conduct;

k. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

229. Typicality: Plaintiffs' claims are typical of those of the other patients of the Class because Plaintiffs, like other Class members, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

230. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Ascension acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Ascension's policies challenged herein apply to and affect Class members uniformly and Plaintiffs' challenges of these policies hinge on Ascension's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

231. Adequacy: Plaintiffs will serve as a fair and effective representative for the Class members, possessing no conflicting interests that would hinder the protection of their rights. The

relief sought by the Plaintiffs aligns with the collective interests of the Class, without any adverse implications for its members. The infringements upon the Plaintiffs' rights and the damages incurred are emblematic of those experienced by other Class members. Moreover, Plaintiffs have engaged legal counsel adept in navigating intricate class action and data breach litigation, demonstrating a commitment to vigorously pursue this case.

232. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Ascension. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

233. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Ascension would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

234. The litigation of the claims brought herein is manageable. Ascension's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

235. Adequate notice can be given to Class members directly using information maintained in Ascension's records.

236. Unless a Class-wide injunction is issued, Ascension may continue in its failure to properly secure the Private Information of Class members, Ascension may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Ascension may continue to act unlawfully as set forth in this Complaint.

237. Further, Ascension has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

238. Similarly, specific issues outlined in Rule 42(d)(1) warrant certification as they entail distinct yet shared concerns pivotal to advancing the resolution of this case and the interests of all parties involved. These issues include, but are not confined to:

a. Whether the Ascension failed to promptly notify both Plaintiffs and the Class about the Data Breach;

b. Whether the Ascension bore a legal responsibility to exercise due diligence in the acquisition, storage, and protection of Private Information belonging to Plaintiffs and the Class;

c. Whether the security measures implemented by Ascension to safeguard their data systems aligned with industry best practices endorsed by data security experts;

d. Whether Ascension's omission of adequate protective security measures amounted to negligence;

e. Whether Ascension neglected to undertake commercially reasonable measures to secure patient Private Information; and

f. Whether adherence to data security recommendations outlined by the FTC, by HIPAA and those advocated by data security experts could have feasibly prevented the occurrence of the Data Breach

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

240. Defendant requires its patients, including Plaintiffs and Class members, to submit non-public Private Information in the ordinary course of providing its services.

241. Ascension gathered and stored the Private Information of Plaintiffs and Class members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

242. Plaintiffs and Class members entrusted Ascension with their private information, expecting that the Ascension would protect and secure it.

243. Ascension had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

244. By voluntarily undertaking the responsibility to collect, store, share, and use this data for commercial gain, Ascension assumed a duty of care to employ reasonable measures to secure and safeguard its computer systems and the Private Information of Class members contained within them. This duty included preventing unauthorized disclosure and protecting the information from theft. Additionally, Ascension was responsible for implementing processes to detect security breaches promptly and to notify affected individuals expeditiously in the event of a data breach.

245. Ascension had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

246. Ascension's duty to use reasonable security measures under HIPAA required Ascension to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

247. Ascension owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Private Information.

248. Ascension's duty to employ reasonable security measures arose from the special relationship between Ascension and the Plaintiffs and Class members. This relationship was established because the Plaintiffs and Class members entrusted Ascension with their confidential private information as a necessary part of being patients.

249. Ascension's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Ascension is bound by industry standards to protect confidential Private Information.

250. Ascension was subject to an "independent duty," untethered to any contract between Ascension and Plaintiffs or the Class.

251. Ascension also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

252. Moreover, Ascension had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

253. Ascension had, and continues to have, a duty to adequately disclose if the private information of the Plaintiffs and Class members in its possession might have been compromised, the manner in which it was compromised, the specific types of data affected, and the timing of the breach. Such notice is necessary to enable the Plaintiffs and Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their private information by third parties.

254. Ascension breached its duties under the FTC Act, HIPAA, and other relevant standards, demonstrating negligence by failing to implement reasonable measures to protect Class

members' Private Information. Specific negligent actions and oversights by the Ascension include, but are not limited to:

a. Failing to implement and maintain reasonable technical and administrative information security controls to safeguard Class members' Private Information.

b. Inadequately monitoring the security of their networks and systems.

c. Allowing unauthorized access to Class members' Private Information.

d. Failing to promptly detect that Class members' Private Information had been compromised.

e. Neglecting to remove Private Information of former patients that was no longer required to be retained according to regulations.

f. Failing to promptly and adequately inform Class members about the occurrence and extent of the Data Breach, preventing them from taking appropriate measures to mitigate the risk of identity theft and other damages.

255. Ascension violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Ascension's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

256. Plaintiffs and Class members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

257. Ascension's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

258. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

259. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Ascension's inadequate security practices.

260. It was foreseeable that Ascension's failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

261. Ascension has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

262. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Ascension knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Ascension's systems or transmitted through third party systems.

263. It was thus foreseeable that the failure to adequately safeguard Class members' Private Information would lead to one or more forms of harm or injury to the Class members.

264. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Ascension's possession.

265. Ascension was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

266. Ascension's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship.

267. Ascension has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

268. But for Ascension's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

269. There is a close causal connection between Ascension's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Ascension's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

270. As a direct and proximate result of Ascension's negligence, Plaintiffs and the Class have suffered and will suffer injury, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains

unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

271. Additionally, as a direct and proximate result of Ascension's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

272. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

273. Plaintiffs and the Class are also entitled to injunctive relief, which should compel the Ascension to: (i) Enhance its data security systems and monitoring procedures; (ii) Undergo annual audits of these systems and monitoring procedures in the future; and (iii) Ensure ongoing provision of sufficient credit monitoring services to all Class members.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

274. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

275. According to the Federal Trade Commission Act, 15 U.S.C. § 45, Ascension was obligated to furnish fair and adequate computer systems and data security practices to protect the private information of both the Plaintiffs and Class members.

276. Ascension's duty to use reasonable security measures under HIPAA required Ascension to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

277. Ascension breached its duties to Plaintiffs and Class members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

278. Ascension's failure to comply with applicable laws and regulations constitutes negligence per se.

279. Plaintiffs and Class members are within the class of persons the statutes were intended to protect and the harm to Plaintiffs and Class members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

280. But for Ascension's wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

281. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Ascension's breach of their duties. Ascension knew or should have known that by failing to meet its duties, Ascension's breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

282. As a direct and proximate result of Ascension's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

283. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

284. Plaintiffs and Class members were required to deliver their Private Information to Ascension as part of the process of obtaining services at Ascension. Plaintiffs and Class members paid money, or money was paid on their behalf, to Ascension in exchange for services.

285. Ascension solicited, offered, and invited Class members to provide their private information as part of its regular business practices. The Plaintiffs and Class members accepted Ascension's request and provided their private information to Ascension.

286. Ascension solicited, offered, and invited Class members to provide their private information as part of its regular business practices. The Plaintiffs and Class members accepted Ascension's request and provided their Private Information to Ascension solicited, offered, and invited Class members to provide their private information as part of its regular business practices.

287. Plaintiffs and the Class entrusted their Private Information to Ascension. In so doing, Plaintiffs and the Class entered into implied contracts with Ascension by which Ascension agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

288. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Ascension's data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

289. Implicit in the agreement between Plaintiffs and Class members and Ascension to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

290. The mutual understanding and intent of Plaintiffs and Class members on the one hand, and Ascension, on the other, is demonstrated by their conduct and course of dealing.

291. On information and belief, at all relevant times Ascension promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

292. On information and belief, Ascension further promised to comply with industry standards and to make sure that Plaintiffs' and Class members' Private Information would remain protected.

293. Plaintiffs and Class members paid money to Ascension with the reasonable belief and expectation that Ascension would use part of its earnings to obtain adequate data security. Ascension failed to do so.

294. Plaintiffs and Class members would not have entrusted their Private Information to Ascension in the absence of the implied contract between them and Ascension to keep their information reasonably secure.

295. Plaintiffs and Class members would not have entrusted their Private Information to Ascension in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

296. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

297. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Ascension.

298. Ascension breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

299. Ascension breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class members and continued acceptance of Private Information and storage of other personal information after Ascension knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

300. As a direct and proximate result of Ascension's breach of the implied contracts, Plaintiffs and Class members sustained damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting

to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

301. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

302. Plaintiffs and the Class are also entitled to injunctive relief requiring the Ascension to: (i) Strengthen its data security systems and monitoring procedures; (ii) Undergo annual audits of these systems and procedures in the future; and (iii) Immediately provide adequate credit monitoring to all Class members.

COUNT IV
Violation of the Missouri Merchandising Practices Act,
Mo. Rev. Stat. § 407.010 *et seq.*
(On Behalf of Plaintiffs and the Class)

303. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

304. The Missouri Merchandising Practice Act (the "MMPA") prohibits false, fraudulent, or deceptive merchandising practices to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services.

305. The MMPA prohibits the "act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

306. The MMPA defines "Merchandise" as "any objects, wares, goods, commodities, intangibles, real estate or services." Mo. Rev. Stat. § 407.010(4).

307. Plaintiffs, individually and on behalf of the Class, are entitled to bring an action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.20, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award the prevailing party attorneys' fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper. Mo. Rev. Stat. § 407.025.

308. Ascension is a "person" within the meaning of the MMPA in that Ascension is a domestic, for-profit corporation. Mo. Rev. Stat. § 407.010(5).

309. Plaintiffs and Class members are "persons" under the MMPA because they are natural persons and they used Ascension's services for personal, family, and/or household use.

310. The Missouri Attorney General has specified the settled meanings of certain terms used in the enforcement of the MMPA. Specifically, Mo. Code Regs. tit. 15, § 60 -8.020, provides:

(1) Unfair practice is any practice which—

(A) Either

1. Offends any public policy as it has been established by the Constitution, statutes, or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive, or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

311. Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also* Restatement, Second, Contracts, sections 364 and 365.

312. Pursuant to the MMPA and Mo. Code Regs. Tit. 15, § 60- 8.020, Ascension's acts and omissions fall within the meaning of "unfair."

313. Ascension engaged in a "trade" or "commerce" within the meaning of the MMPA with regard to services which are supposed to keep Plaintiffs' and the Class members' Private Information safe and secure.

314. Ascension engaged in unlawful practices and deceptive conduct, which emanated from its Missouri headquarters, in violation of the MMPA by omitting and/or concealing material facts related to the safety and security of Plaintiffs' and the Class members' Private Information. Ascension's unfair and unethical conduct of failing to secure Private Information and failing to disclose the Data Breach caused substantial injury to consumers in that the type of consumers' personal information impacted by the breach can be used to orchestrate a host of fraudulent activities, including medical, insurance, and financial fraud and identity theft. The impacted consumers have been placed in an immediate and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach.

315. Ascension's conduct of failing to secure data required Plaintiffs and the Class to undertake time-consuming, and often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Private Information.

316. Ascension's conduct of concealing, suppressing, or otherwise omitting material facts regarding the Data Breach was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MMPA.

317. By failing to secure sensitive data and failing to disclose and inform Plaintiffs and Class members about the Breach of Private Information, Ascension engaged in acts and practices that constitute unlawful practices in violation of the MMPA. Mo. Ann. Stat. §§ 407.010, *et seq.*

318. Ascension engaged in unlawful practices and deceptive conduct in the course of their business that violated the MMPA including misrepresentations and omissions related to the safety and security of Plaintiffs' and the Class's Private Information. Mo. Rev. Stat. § 407.020.1.

319. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Class member suffered actual harm in the form of money and/or property because the disclosure of their Private Information has value encompassing financial data and tangible money.

320. Ascension's "unfair" acts and practices include:

a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Plaintiffs and Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' personal information; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

321. Ascension's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' personal information, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

322. Ascension's misrepresentations and omissions were material to consumers and made in order to induce consumers' reliance regarding the safety and security of Private Information in order to obtain consumers' Private Information and purchase of medical products and/or services.

323. Ascension's deceptive practices misled Plaintiffs and the Class and would cause a reasonable person to enter into transactions with Ascension that resulted in damages.

324. As such, Plaintiffs and the Class seek: (1) to recover actual damages sustained; (2) to recover punitive damages; (3) to recover reasonable attorneys' fees and costs; and (4) such equity relief as the Court deems necessary or proper to protect Plaintiffs and the members of the Class from Ascension's deceptive conduct and any other statutorily available damages or relief the court deems proper.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

325. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

326. Additionally or in the alternative, Plaintiffs bring this claim for unjust enrichment.

327. Plaintiffs and Class members conferred a monetary benefit on Ascension. Specifically, they paid Ascension and/or its agents for the provision of services and in so doing also provided Ascension with their Private Information. In exchange, Plaintiffs and Class members should have received from Ascension the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

328. Ascension knew that Plaintiffs and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Ascension profited from Plaintiffs' retained data and used Plaintiffs' and Class members' Private Information for business purposes.

329. Ascension failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not fully compensate Plaintiffs or Class members for the value that their Private Information provided.

330. Ascension acquired the Private Information through inequitable record retention, having failed to investigate and/or disclose the inadequate data security practices previously mentioned.

331. If Plaintiffs and Class members had known that Ascension would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Ascension or obtained services at Ascension.

332. Plaintiffs and Class members have no adequate remedy at law.

333. Ascension enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Ascension instead calculated to increase its own profit at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Ascension's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

334. Under the circumstances, it would be unjust for Ascension to be permitted to retain any of the benefits that Plaintiffs and Class members conferred upon it.

335. As a direct and proximate result of Ascension's conduct, Plaintiffs and Class members have suffered and will suffer injury, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting

to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Ascension's possession and is subject to further unauthorized disclosures so long as Ascension fails to undertake appropriate and adequate measures to protect the Private Information.

336. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Ascension and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Ascension from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

337. Plaintiffs and Class members may not have an adequate remedy at law against Ascension, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
Violation of the Arkansas Deceptive Trade Practices Act,
A.C.A. §§ 4-88-101, *et seq.*
(On Behalf of Plaintiff Dunn and the Arkansas Subclass)

338. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

339. Alternatively or in addition, Plaintiff Dunn and the Arkansas Subclass members bring this claim for violation of Arkansas's Deceptive Trade Practices Act, A.C.A. §§ 4-88-101, *et seq*.

340. Ascension is a "person" as defined by A.C.A. § 4-88-102(5).

341. Ascension's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

342. Ascension advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

343. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

344. Ascension engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;

b. Advertising goods or services with the intent not to sell them as advertised;

c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;

d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and

e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

345. Ascension's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Dunn's and Arkansas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110- 104(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Dunn's and Arkansas Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dunn's and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq*., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110- 104(b).

346. Ascension's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Ascension's data security and ability to protect the confidentiality of consumers' Private Information.

347. Ascension intended to mislead Plaintiff Dunn and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

348. Had Ascension disclosed to Plaintiff Dunn and Arkansas Subclass members that its data systems were not secure and, thus, vulnerable to attack, Ascension would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Ascension accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Plaintiff Dunn and the Arkansas Subclass members acted reasonably in relying on Ascension's misrepresentations and omissions, the truth of which they could not have discovered.

349. Ascension acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Dunn's and Arkansas Subclass members' rights.

350. As a direct and proximate result of Ascension's unconscionable, unfair, and deceptive acts or practices and Plaintiff Dunn's and Arkansas Subclass members' reliance thereon, Plaintiff Dunn and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

351. Plaintiff Dunn and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VII
Violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff Brown and the Florida Subclass)

352. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

353. Alternatively or in addition, Plaintiff Brown and Florida Subclass members bring this claim for violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*.

354. At all times relevant herein, Plaintiff Brown and the Florida Subclass members are "consumers" as defined under Fla. Stat. § 501.203(7).

355. Ascension, while operating its healthcare facilities in Florida, engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the conduct of "trade or commerce" (as defined in the Florida Deceptive and Unfair Trade Practices Act, Fla. Sat. § 501.203), in violation of Fla. Sat. § 501.203, including the following:

a. Ascension misrepresented and fraudulently advertised material facts to Plaintiff Brown and the Florida Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Brown's and the Florida Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Ascension misrepresented and fraudulently advertised material facts to Plaintiff Brown and the Florida Subclass by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Brown's and the Florida Subclass members' Private Information;

c. Ascension omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff Brown's and the Florida Subclass members' Private Information;

d. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff Brown's and the Florida Subclass members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data

Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45 and Fla. Stat. § 501.171.

e. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff Brown and Florida Subclass members in a timely and accurate manner, contrary to the duties imposed by Fla. Stat. § 501.171;

f. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Brown's and the Florida Subclass members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

356. As a direct and proximate result of Ascension's deceptive trade practices, Plaintiff Brown and Florida Subclass members suffered an ascertainable loss of money or property, real or personal, as described above, including the payment for purchases they otherwise would not have made or overpayment for the purchases they did make and the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

357. The above unfair and deceptive practices and acts by Ascension were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

358. Ascension knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff Brown's and the Florida Subclass members' Private Information and that risk of a data breach or theft was highly likely. Ascension's

actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Brown and the Florida Subclass.

359. Florida Class Members seek relief under Fla. Stat. § 501.201 et seq., including damages, statutory damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs pursuant to Fla. Stat. § 501.2105.

COUNT VIII
Violation of the Indiana Deceptive Consumer Sales Act,
Ind. Code §§ 24-5-0.5-0.1, *et seq.*
(On Behalf of Plaintiff Pitchers and the Indiana Subclass)

360. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

361. Alternatively or in addition, Plaintiff Pitchers and Indiana Subclass members bring this claim for violation of Indiana's Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3(a) ("IDCSA"), which prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

362. Ascension is a "supplier" of consumer services as provided by Ind. Code § 24-5-0.5-2. Plaintiff Pitchers and Indiana Subclass members are "consumers" of Ascension's services.

363. Ascension engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions," in violation of the IDCSA. As a regular part of its business, Ascension operates health care facilities in Indiana. It accepts payments from customers, like Plaintiff Pitchers and the Indiana Subclass members, for Ascension services and medical supplies. On information and belief, consumer transactions were processed in Indiana and health care services were performed in Indiana.

364. In connection with its consumer transactions, Ascension engaged in unfair, abusive or deceptive acts, omissions or practices by, inter alia, engaging in the following conduct:

a. failing to maintain sufficient security to keep Plaintiff Pitchers's and the Indiana Subclass members' Private Information from being hacked and stolen;

b. misrepresenting material facts to Plaintiff Pitchers and the Indiana Subclass members, in connection with providing health care services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Pitchers's and the Indiana Subclass members' Private Information as contained in its Privacy Policy;

c. misrepresenting material facts to Plaintiff Pitchers and the Indiana Subclass members, in connection with providing health care services, by representing that Ascension did and would comply with the requirements of relevant federal and state law pertaining to the privacy and security of Plaintiff Pitchers's and the Indiana Subclass members' Private Information, such requirements included, but are not limited to, those imposed by laws such as the Federal Trade Commission Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Pitchers's and the Indiana Subclass members' Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

365. Ascension knew that its computer systems and data security practices were inadequate to safeguard Plaintiff Pitchers's and the Indiana Subclass members' Private

Information and that risk of a data breach or theft was highly likely. Nevertheless, it did nothing to warn Plaintiff Pitchers and the Indiana Subclass members about its data insecurities, and instead affirmatively promised that it would maintain adequate security. This was a deliberate effort to mislead consumers, such as Plaintiff Pitchers and the Indiana Subclass members, in order to encourage them to receive health care services even while Ascension knew that its consumers' sensitive Private Information was vulnerable.

366. The above unfair and deceptive practices and acts or omissions by Ascension were done as a part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

367. As a direct and proximate result of Ascension’s deceptive trade practices, Plaintiff Pitchers and the Indiana Subclass members suffered damages and injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

368. As a direct and proximate result of Ascension's deceptive trade practices, Plaintiff Pitchers and the Indiana Subclass members are now likely to suffer identity theft crimes and face a lifetime risk of identity theft crimes.

369. Plaintiff Pitchers and the Indiana Subclass members seek relief under Ind. Code § 24-5-0.5-4, including damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

370. Plaintiff Pitchers and the Indiana Subclass members injured by Ascension’s unfair and deceptive trade practices also seek treble damages pursuant to Ind. Code § 24-5-0.5-4(i).

COUNT IX
Violation of the Protection of Consumer Information,
Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*
(On Behalf of Plaintiff Rutherford and the Kansas Subclass)

371. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

372. Alternatively or in addition, Plaintiff Rutherford and Kansas Subclass members bring this claim for violation of Kansas's statute on the Protection of Consumer Information.

373. Ascension is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

374. Plaintiff Rutherford's and Kansas Subclass members' Private Information (e.g., Social Security numbers) includes "Personal Information" as covered under Kan. Stat. Ann. § 50-7a02(a).

375. Ascension is required to accurately notify Plaintiff Rutherford and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff Rutherford's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

376. Because Ascension was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiff Rutherford's and Kansas Subclass members' Personal Information, Ascension had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50- 7a02(a).

377. By failing to disclose the Data Breach in a timely and accurate manner, Ascension violated Kan. Stat. Ann. § 50-7a02(a).

378. As a direct and proximate result of Ascension's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff Rutherford and Kansas Subclass members suffered damages, as described above.

379. Plaintiff Rutherford and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT X
Violation of Kansas Consumer Protection Act,
K.S.A. §§ 50-623, *et seq.*
(On Behalf of Plaintiff Rutherford and the Kansas Subclass)

380. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

381. Alternatively or in addition, Plaintiff Rutherford and Kansas Subclass members bring this claim for violation of the Kansas Consumer Protection Act.

382. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

383. Plaintiff Rutherford and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

384. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

385. Ascension is a "supplier" as defined by K.S.A. § 50-624(l).

386. Ascension advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

387. Ascension engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Rutherford's and Kansas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rutherford's and Kansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50- 6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Rutherford and Kansas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rutherford's and Kansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rutherford's and Kansas Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rutherford and Kansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50- 6,139b.

388. Ascension's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Ascension's data security and ability to protect the confidentiality of consumers' Private Information.

389. Ascension intended to mislead Plaintiff Rutherford and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

390. Had Ascension disclosed to Plaintiff Rutherford and Class members that its data systems were not secure and, thus, vulnerable to attack, Ascension would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Ascension accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Plaintiff Rutherford and the Kansas Subclass members acted reasonably in relying on Ascension's misrepresentations and omissions, the truth of which they could not have discovered.

COUNT XI
Violation of the Oklahoma Consumer Protection Act,
Okla. Stat. Ann. tit. 15, § 751, *et seq.*
(On Behalf of Plaintiff Hayes and the Oklahoma Subclass)

391. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

392. Alternatively or in addition, Plaintiff Hayes and Oklahoma Subclass members bring this claim for violation of the Oklahoma Consumer Protection Act.

393. The purchases of healthcare services and medical supplies from Ascension by Plaintiff Hayes and the members of the Oklahoma Subclass constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752.

394. Ascension engaged in unlawful, unfair, and deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale of healthcare services and medical supplies to Plaintiff Hayes and the Oklahoma Subclass members in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Ascension knowingly, or with reason to know, misrepresented material facts pertaining to the sale of medical services and supplies to Plaintiff Hayes and the Oklahoma Subclass members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Hayes's and the Oklahoma Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft in violation of Okla. Stat. tit. 15, § 753(5) and (8);

b. Ascension knowingly, or with reason to know, misrepresented material facts pertaining to the sale of medical supplies and services to Plaintiff Hayes and the

Oklahoma Subclass members by representing that Ascension did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Hayes's and the Oklahoma Subclass members' Private Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);

c. Ascension omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff Hayes's and the Oklahoma Subclass members' Private Information in violation of Okla. Stat. tit. 15, § 753(5) and (8);

d. Ascension engaged in unfair, unlawful, and deceptive trade practices with respect to the sale of medical services and supplies by failing to maintain the privacy and security Plaintiff Hayes's and the Oklahoma Subclass members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including 15 U.S.C. § 45 and Okla. Admin. Code §§ 365:35-1-40, 365:35-1-20;

e. Ascension engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of medical services and supplies by failing to disclose the Data Breach to Plaintiff Hayes and the Oklahoma Subclass members in a timely and accurate manner, in violation of 24 Okla. Sta. Ann. § 163(A);

f. Ascension engaged in unlawful, unfair, and deceptive trade practices with respect to the sale of medical supplies and services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and

protect Plaintiff Hayes's and the Oklahoma Subclass members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

395. The above unlawful, unfair, and deceptive trade practices and acts by Ascension were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

396. As a direct and proximate result of Ascension's deceptive acts and practices, Plaintiff Hayes and Oklahoma Subclass members suffered injury and/or damages.

397. Plaintiff Hayes and Oklahoma Subclass members seek relief under Okla. Stat. Ann. tit. 15, § 761.1 including injunctive relief, actual damages, and attorneys' fees and costs.

COUNT XII
Breach of Confidentiality of Health Records,
Wis. Stat. § 146.81, *et seq.*
(On Behalf of Plaintiff Farrand and the Wisconsin Subclass)

398. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

399. Alternatively or in addition, Plaintiff Farrand and Wisconsin Subclass members bring this claim for Breach of Confidentiality pf Patient Health Records, pursuant to Wis. Stat. §§ 146.81, *et seq.*, which states: "All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient." Wis. Stat. § 146.82(1).

400. The stolen Private Information belonging to Plaintiff Farrand and the Wisconsin Subclass are "Health care records" under Wis. Stat. § 146.81(4).

401. Ascension violated Wis. Stat. §§ 146.81, et seq. when it compromised, allowed access to, released, and disclosed patient health care records and PHI to third parties without the informed consent or authorization of Plaintiff Farrand and the members of the Wisconsin Subclass. Ascension did not and does not have express or implied consent to disclose, allow access to, or release Plaintiff Farrand's and Wisconsin Subclass members' Private Information. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiff Farrand and the members of the Wisconsin Subclass when it told them their Private Information would be private and secure.

402. Ascension did not disclose to or warn Plaintiff Farrand and Wisconsin Subclass members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Ascension's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiff Farrand and Wisconsin Subclass members did not know or expect, or have any reason to know or suspect, that Ascension's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiff Farrand and Wisconsin Subclass members, and on Ascension's website.

403. Wis. Stat. § 146.84(1)(b) states,

> Any person, including the state or any political subdivision of the state, who violates Wis. Stat. s. 146.82 or 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable actual attorney fees.

404. Wis. Stat. § 146.84(1)(bm) states,

> Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to any

> person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $1,000 and costs and reasonable actual attorney fees." Wis. Stat. § 146.84(1)(bm).

405. Wis. Stat. § 146.84(1)(c) states,

> An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

406. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. § 146.81. A simple comparison of other Wisconsin statues (e.g., Wis. Stat. § 134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. § 146.84 when it explicitly did so in other privacy statutes. *See* Wis. Stat. § 134.97(3)(a) and (b).

407. Similarly, the Wisconsin Legislature made it clear that the exemplary damages referred to in Wis. Stat. § 146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statue (Wis. Stat. § 895.043(2), "Scope" of punitive damages), specifically and unequivocally excludes an award of "exemplary damages" under Wis. Stat. §§ 146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043.19. In short, exemplary damages under Wis. Stat. § 146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been "injured" as a result of a negligent data breach like the one at issue here.

408. Plaintiff Farrand and Wisconsin Subclass members request that the Court issue declaratory relief declaring Ascension's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PHI data between Ascension and third parties unlawful. Plaintiff Farrand and Wisconsin Subclass

members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PHI without first adequately securing or encrypting it.

409. Plaintiff Farrand and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by Wis. Stat. § 146.84(1)(bm), including injunctive relief and attorneys' fees.

COUNT XIV
Violation of Wisconsin Deceptive Trade Practices Act,
Wis. Stat. §§ 100.18, *et seq.*
(On Behalf of Plaintiff Farrand and the Wisconsin Subclass)

410. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

411. Alternatively or in addition, Plaintiffs allege that Ascension's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. § 100.18 (the "WDTPA"), which provides that:

> [no] "firm, corporation or association … with intent to sell, distribute, increase the consumption of … any … merchandise … directly or indirectly, to the public for sale … shall make, publish, disseminate, circulate, or place before the public … in this state, in a … label … or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public … which … contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

412. Plaintiff Farrand and Wisconsin Subclass members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

413. Ascension violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the

Data Breach, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; and (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access.

414. The purpose of Ascension's misrepresentations set forth herein was to ensure that Plaintiff Farrand and Wisconsin Subclass members would entrust Ascension with their data, thereby increasing the sales and use of Ascension's goods and services.

415. Ascension knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breach and theft was high. Ascension's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Farrand and Wisconsin Subclass members.

416. Plaintiff Farrand and Wisconsin Subclass members relied upon Ascension's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

COUNT XIV
Violation of Notice of Unauthorized Acquisition of Personal Information, Wis. Stat. §§ 134.98(2), *et seq*.
(On Behalf of Plaintiff Farrand and the Wisconsin Subclass)

417. Plaintiffs re-allege and incorporate by reference every allegation in the preceding paragraphs as if fully set forth herein.

418. Alternatively or in addition, Plaintiff Farrand and the Wisconsin Subclass allege that Ascension's conduct violates Wisconsin's statute regarding Notice of Unauthorized Acquisition of Personal Information, Wis. Stat. §§ 134.98(2), *et seq*.

419. Ascension is a business that maintains or licenses "Personal Information" Plaintiff Farrand's and Wisconsin Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

420. Ascension is required to accurately notify Plaintiff Farrand and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person whom it has not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

421. Because Ascension knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Ascension had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

422. By failing to disclose the Ascension data breach in a timely and accurate manner, Ascension violated Wis. Stat. § 134.98(2).

423. As a direct and proximate result of Ascension's violations of Wis. Stat. § 134.98(3)(a), Plaintiff Farrand and Wisconsin Subclass members suffered damages, as described above.

424. Plaintiff Farrand and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief. as defined by Wis. Stat. § 134.98(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiffs as class representative, and Plaintiffs' counsel as Class Counsel;

B. That the Court grant equitable relief enjoining Ascension from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class members;

C. That the Court grant injunctive relief requested by Plaintiff, including injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including an order:

i. requiring Ascension to conduct regular database scanning and securing checks;

ii. requiring Ascension to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

iii. requiring Ascension to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

iv. requiring Ascension to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Ascension's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

v. requiring Ascension to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

vi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Ascension's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. That the Court award Plaintiffs and Class members damages, including actual, nominal, statutory, consequential, and punitive damages, for each cause of action as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Ascension as a result of its unlawful acts, omissions, and practices;

F. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorney's fees, costs, and expenses;

G. That the Court award pre-and post-judgment interest at the maximum legal rate; and

H. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all claims so triable.

Date: June 21, 2024

Respectfully submitted,

/s/ Norman E. Siegel
Norman E. Siegel (44378 MO)
J. Austin Moore (64040 MO)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

David M. Berger *
Linda P. Lam*
Sarah E. Hillier*
GIBBS LAW GROUP LLP
1111 Broadway, Ste. 2100
Oakland, CA 94607
Tel: 510-350-9700
dmb@classlawgroup.com
lpl@classlawgroup.com
seh@classlawgroup.com
**pro hac vice application forthcoming*

Counsel for Plaintiffs and the Proposed Class